FCC PREPAREDNESS

for MAJOR PUBLIC EMERGENCIES

CHAIRMAN'S 30 DAY REVIEW

prepared by the PUBLIC SAFETY AND HOMELAND SECURITY BUREAU

SEPTEMBER 2009

TABLE OF CONTENTS

FCC PREPAREDNESS FOR A MAJOR PUBLIC EMERGENCY

CHAIRMAN'S REVIEW

EXECUTIVE SUMMARY

This report responds to the June 30, 2009, request from Chairman Genachowski to the Public Safety and Homeland Security Bureau for an analysis and briefing within thirty days on the FCC's preparedness for a major public emergency.[1]

During a major public emergency, the FCC's primary mission is to ensure continuous operations and reconstitution of critical communications systems and services. This mission statement was developed after lengthy analysis by an in-house FCC team. It describes the essential work that is performed by the FCC during emergency situations that is in direct support of one or more of the National Essential Functions. It was reviewed by an external Interagency Board, and on June 1, 2009, it was approved by John Brennan, Assistant to the President for Homeland Security and Counterterrorism.

In developing this mission, the FCC's Bureaus and Offices identified more than 140 functions that need to be performed during an emergency, or need to be resumed as quickly as possible after being suspended during a disaster.

Within the FCC the Public Safety and Homeland Security Bureau (PSHSB) serves as the lead coordinator for the FCC's National Security and Emergency Preparedness planning and response activities. The Office of Managing Director (OMD) and Enforcement Bureau (EB) also have major responsibilities for the FCC's emergency planning and response efforts. OMD provides the necessary IT, communications, physical, and financial resources to implement the emergency plans. EB provides essential field staff and management personnel for emergency deployments in disaster areas. Beyond that, virtually every Bureau and Office plays an important role and is actively engaged in the emergency planning and response efforts: their expertise and efforts are critical to the effective completion of the FCC's emergency mission.

The FCC also works with its Federal partners and the communications sector in ensuring continuous operations and reconstitution of critical communications systems and services. FCC staff members actively serve on several Federal emergency preparation and response teams and working groups where much of this work is accomplished. The vast majority of the Nation's critical communications assets are owned and operated by the private sector. Accordingly, the FCC works closely with the communications sector to assess the operational status of essential communications systems and assist in the restoration of these critical assets and related services.

Specifically, the FCC takes the following actions when an emergency is declared:

[1] *See* http://www.fcc.gov/pshs/docs/memo.pdf for a copy of this memorandum. In addition, there is a briefing process for incoming FCC leadership to inform it of its roles, responsibilities, and other key functions during a major public emergency.

- Ensures the safety and security of FCC employees.
- Protects essential FCC equipment, records, and other assets.
- Reaches out to 9-1-1 centers and the public safety community to determine their operational status and needs.
- Reaches out to and gathers operational information from its licensees and regulated entities, especially key Emergency Alert Systems stations.
- Uses specialized equipment to identify and resolve communications disruptions.
- Conducts analysis of communication systems and operations.
- Provides timely and actionable disaster-related information to the National Communications System, the Federal Emergency Management Agency, the Joint Telecommunications Resources Board, and other Federal emergency managers.
- Deploys expert personnel as liaison officers and responders in the field.
- Issues emergency authorizations and waives rules to expedite restoration of essential communications services.
- Coordinates use of spectrum for emergency response.
- Coordinates cross-border, undersea cable, and orbital spectrum issues.

Over the past five years, the FCC has successfully responded to several emergencies and disasters in which essential communications systems sustained severe damage. In addition, PSHSB has substantially improved the FCC's emergency plans, developed a number of important innovative systems and programs that improve the FCC's capability to respond to emergencies, and conducted training and exercises to ensure that all FCC emergency response personnel understand their roles during emergencies.

While the FCC has shown that it is prepared to respond to communications emergencies and perform its mission, PSHSB has identified a number of areas in which the FCC can improve its emergency planning and response, among them:

- Expand our cyber security expertise.
- Expand public safety and emergency response outreach activities.
- Enhance the capacity and capability of emergency personnel for remote access to essential FCC applications and databases.
- Expand emergency response and continuity training.
- Modernize the disaster outage and Priority Services programs.

SECTION 1: FCC'S EMERGENCY MANAGEMENT PLAN

1. Describe the FCC's emergency management plan, including:
   - FCC's main functions during a crisis:
     - Crises affecting significant communications infrastructure
     - Crises affecting FCC/government continuity of operations
   - Organization, roles and responsibilities, chain of command
   - Interfaces/relationships with outside groups, such as:
     - FEMA, other federal agencies, state and local agencies
     - Telecommunications service providers
     - Other critical infrastructure providers
   - Command-and-control infrastructure (including backup redundancies)
     - Operations centers
     - Field agents
     - Lines of communication

I. FCC'S PRIMARY MISSION DURING A CRISIS

During an emergency, the FCC's function is to ensure continuous operations and reconstitution of critical communications systems and services. This mission statement was developed after lengthy analysis by an in-house FCC team and reviewed by an external Interagency Board.

Specifically, the FCC takes the following actions to facilitate critical communications and services during an emergency affecting significant communications infrastructure:

- Ensures the safety and security of FCC employees.
- Protects essential FCC equipment, records, and other assets.
- Reaches out to 9-1-1 centers and the public safety community to determine their operational status and needs.
- Reaches out to and gathers operational information from its licensees and regulated entities, especially key Emergency Alert Systems stations.
- Conducts analysis of communication systems and operations.
- Uses specialized equipment to identify and resolve communications disruptions.
- Provides timely and actionable disaster-related information to the National Communications System, the Federal Emergency Management Agency, and the Joint Telecommunications Resources Board, and others.

- Deploys expert personnel as liaison officers and responders in the field.[2]
- Issues emergency authorizations and waives rules to expedite restoration of essential communications services.
- Coordinates use of spectrum for emergency response.
- Coordinates cross-border, undersea cable, and orbital spectrum issues.

II. FCC CONTINUITY OF OPERATIONS

The FCC's plans for emergency management follows an All Hazards approach to Continuity of Operations, including cyber attacks, pandemics, and delegation and devolution of leadership.

The FCC's Continuity of Operations or COOP plan identifies the functions, operations, and resources necessary for the FCC to perform its mission under all circumstances, including any emergency or other event that requires the FCC to relocate from its headquarters. If operations at FCC headquarters are significantly impaired, essential FCC personnel will relocate to the FCC's COOP site. Facilities, data access and communications are available at the COOP site for the FCC to continue its mission.

The FCC's COOP plan is designed to satisfy several basic objectives including:

- Ensuring the safety and security of FCC employees and others on-site during an emergency.
- Protecting essential equipment, records, and other assets.
- Mitigating risks by identifying requirements before an emergency occurs.
- Facilitating decision-making during a potential or actual emergency.
- Facilitating an orderly recovery from emergency operations.

The Public Safety and Homeland Security Bureau (PSHSB) has the lead role for developing and implementing the FCC's COOP Plan. The Office of Managing Director (OMD) has management responsibility for the logistics for COOP (e.g., facilities, operations, and security) and manages the FCC's network operations.

In addition to the FCC COOP plan, there are individual COOP plans for the Chairman and Commissioners (which PSHSB prepares), and for each Bureau and Office, including the Enforcement Bureau's (EB) field offices. As new leadership comes on board, members receive briefings on the FCC's emergency preparedness and response mission, along with their own respective functions, roles, and responsibilities. Further, they are provided with emergency communications devices and a briefing on operating protocols.

Pandemic Plan The FCC's Pandemic Plan contemplates that absenteeism may be an issue, social distancing may become a requirement, medicine may be in short supply, and large-scale teleworking may be necessary for the FCC to perform its mission. Over the past year, extensive

[2] In addition to providing support for the FCC's emergency response activities, EB field offices routinely and independently respond to events affecting significant communications infrastructure, primarily to address interference concerns that arise from a crisis, incident, or natural disaster.

work has been completed on pandemic planning in response to updated White House directives and the H1N1 outbreak.

Delegation and Devolution Plans The FCC has identified lines of succession among Commissioners and Bureaus and Offices. Further, should a catastrophic event incapacitate FCC leadership in the National Capital Region, the FCC has a Devolution Plan whereby successors from the FCC's field could perform the FCC's mission.

III. ORGANIZATION, ROLES, RESPONSIBILITIES, AND CHAIN OF COMMAND

Responsibility for the FCC's emergency response activities comes, primarily, from the Chairman, Defense Commissioner, Public Safety and Homeland Security Bureau Chief, and the Managing Director.

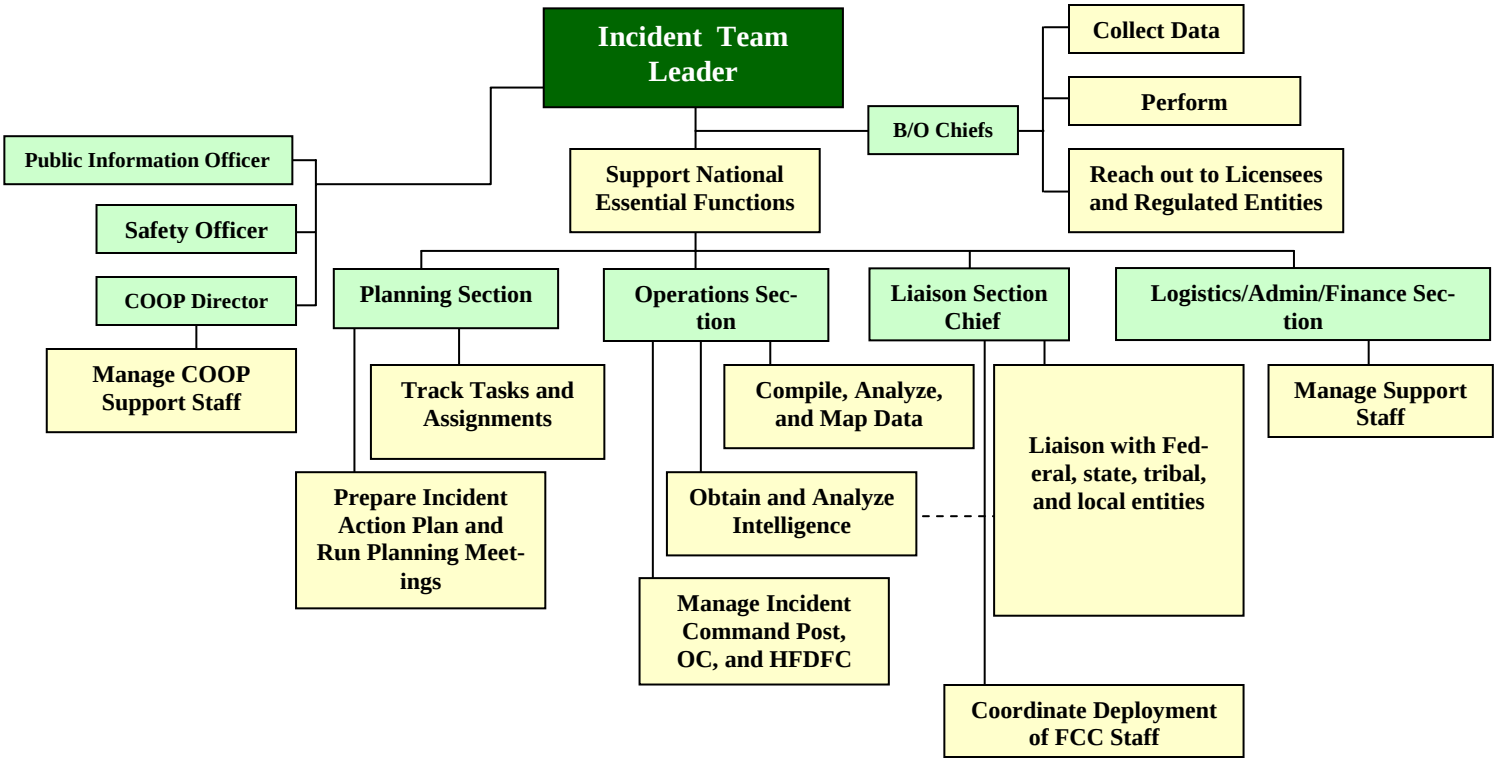
PSHSB has the lead role for developing and implementing the FCC's emergency response plans. OMD has management responsibility for the infrastructure (e.g., facilities, logistics, and security) and manages the FCC's network operations.

The FCC's emergency response plans are scalable from the Division, Bureau, and then agency-level depending on the severity of the emergency and its relevance to communications.

For small scale events that do not affect FCC operations, such as those causing minor damage and little or no loss of life, PSHSB's Public Communications Outreach and Operations Division manages the event. EB field offices also assist in the response to events that occur within their geographic area of responsibility. As the scope and scale of the event grows, PSHSB reaches out to the other Bureaus and Offices. They provide liaison support and contact licensees and regulated entities under their jurisdiction. PSHSB manages these mid-level events and coordinates actions with the Chairman's Office. For major events, like Hurricane Katrina, the Chairman's Office coordinates the FCC's response through the Bureau and Office Chiefs with assistance from PSHSB. Some of these events may rise to such a level that the President issues a Disaster Declaration.

PSHSB provides emergency communications response, coordination, and support for deployed FCC personnel, the Federal Emergency Management Agency (FEMA) and other Federal partners through a multi-discipline Incident Management Team. The Incident Management Team (IMT) consists of an Incident Team Manager, and chiefs of Liaison, Logistics/Administrative/Finance (as needed), Operations, and Planning sections. The team is primarily composed of PSHSB personnel, but also is staffed and supported by representatives from other Bureaus and Offices. The IMT is organized to manage and coordinate the FCC's response and focuses on outreach and assistance to the FCC's licensees and regulated entities.

The organization chart below details the FCC's IMT structure.



IV. INTERFACES / RELATIONSHIPS WITH OUTSIDE GROUPS

A. FEDERAL PARTNERS

The FCC works with its Federal partners and with the communications sector in ensuring continuous operations and reconstitution of critical communications systems and services. These efforts support effective communications for Federal emergency management, first responders, and the public.[3]

FCC staff members are assigned to FEMA's Incident Management Assistance Teams (IMATs). These teams include the first Federal responders into a disaster area. They provide an initial assessment of the communications situation and a forward presence to manage a coordinated Federal response. FCC staff members also are assigned to the Emergency Support Function #2 – Communications team (ESF # 2), which is led by the National Communications System (NCS) and includes the Department of Agriculture, Department of Commerce (National Telecommunications and Information Administration (NTIA)), Department of Defense, Department of Homeland Security, Department of Interior, FCC, Federal Emergency Management Agency (FEMA), and General Services Administration (GSA). The ESF # 2 team is charged with overseeing Fed-

[3] *See* http://www.fcc.gov/pshs/docs/liaison.pdf for a listing of the FCC's homeland security liaison activities.

eral emergency communications response efforts during major disasters under the *National Response Framework.*[4]

B. COMMUNICATIONS SECTOR

The vast majority of the Nation's critical communications assets are owned and operated by the private sector. As a result, the FCC must work closely with the communications sector to assess the operating status of essential communications systems to develop situational awareness that will assist in the restoration of these critical assets and related services.

One of the primary tools the FCC developed to assist in this area is the Disaster Information Reporting System (DIRS). DIRS is a web-based information system through which the FCC collects operational status and restoration information directly from communications providers whose infrastructure is impaired. DIRS provides detailed, end-of-day critical infrastructure and service outage information for wireline and wireless telecommunications services, cable systems, and broadcasters. Participation in the DIRS process is voluntary and all data collected is accorded confidential treatment.

When DIRS is activated, PSHSB sends e-mail notifications to all DIRS users and issues a Public Notice advising other stakeholders. These notifications contain information about the DIRS activation, including the geographic area covered. Participating communications providers supply daily information about their infrastructure status. Based on the information received in DIRS, PSHSB provides daily reports, including maps and charts, and trends. These daily reports form the core of situational awareness reports provided to the White House, FEMA, NCS, and the field.

PSHSB staff has been working to increase the number of telecommunications carriers that are registered in DIRS. Before DIRS was launched, PSHSB staff members led large training events for telecommunications carriers. PSHSB staff members also worked with telecommunications carrier associations to make data collection information available to their members via their web sites. These efforts included collaboration with the National Exchange Carrier Association, which manages the distribution of interstate access revenues between local exchange carriers (LECs) and interexchange carriers. This collaboration has provided PSHSB with contact information for virtually every LEC in the U.S.

The International Bureau (IB) employs an extensive outreach process involving the Satellite Industry Association (SIA) generally, and the specific satellite operators that may be impacted during a hurricane. For example, during Hurricanes Gustav and Ike, IB staff (1) determined the potential impact of the disaster on earth station infrastructure based on demographic information in IB's licensing database; (2) contacted those operators to provide IB point-of-contact information in case the operators required a Special Temporary Authority (STA); (3) established regular communications and status follow up with the satellite service providers and earth station operators in the affected areas; (4) forwarded requests for assistance from the providers and operators to NCS through PSHSB; (5) prepared and issued streamlined STAs for service to the affected areas; and (6) coordinated service requests with Executive Branch agencies when necessary.

[4] *See* ESF # 2 Annex to the National Response Framework at http://www.fema.gov/emergency/nrf/index.htm.

Over the past few years, the Media Bureau developed and employed a multi-part process for information sharing, resource coordination, and assistance delivery with broadcasters during emergencies.[5] The National Association of Broadcasters (NAB) and the system of state broadcast associations provide an extensive base of contact information on commercial broadcasters and an efficient network for information sharing. National Public Radio has provided similar information from its member stations. These entities provide radio facility locations and contact information, and generate spread sheets to track operational developments on a market-specific basis. Finally, they have well-established contacts with both radio and television group owners and their legal and technical representatives, and use these contacts for information collection and dissemination. For cable, the contacts are with the industry groups NCTA (National Cable and Telecommunications Association) and ACA (American Cable Association). For large multiple system operators (MSOs) such as Comcast, Cox and Time Warner, there are contact points that have been coordinated at the national-level. For individual cable system contacts, information comes from NCTA, ACA, the MSOs, contact points from registrations and other filings, and, if necessary, the Internet.

The Wireline Competition Bureau, for example, maintains several databases of telecommunications-provider contact information and has worked extensively on outreach efforts directed at incumbent LECs, competitive LECs, and other providers during emergencies.

The other Bureaus and Offices have similar contacts with their respective licensees, regulated entities, and industry trade groups. Another avenue of reaching out to critical public safety entities and to those relying on their services is through PSHSB's Outreach Program.[6]

V. COMMAND-AND-CONTROL INFRASTRUCTURE

A. OPERATIONS CENTER

The FCC Operations Center is the FCC's 24/7 point of contact for Federal state, tribal, and local entities and public safety organizations. It accomplishes its situational awareness responsibilities by monitoring and compiling information from government agencies, contract alert providers, open media, and private sector sources around the clock. A back-up Operations Center is activated whenever a significant threat to the FCC's headquarters Operations Center is identified.

During disasters and in conjunction with National Special Security Events (NSSE), the FCC's Operations Center collects and analyzes information regarding the status of national security operations, public safety entities, and critical infrastructure-related FCC licensees and regulated entities that may be impacted by these events.

The FCC Operations Center maintains contact with all EB field offices and provides dispatch and coordination of public safety interference complaints, disaster analysis, and deployment communications. EB field offices investigate and resolve these cases.

[5] PSHSB also works with the NAB, NCTA, and other media organizations to increase the number of media companies that participate DIRS.

[6] *See* http://www.fcc.gov/pshs/docs/outreach.pdf for an overview of the PSHSB's outreach activities.

B. FIELD AGENTS

EB field agents who have volunteered for emergency response duties are deployed and report to FEMA at a Joint Field Office (JFO) in the region of the event. Approximately forty EB field agents are trained to support basic emergency response responsibilities in accordance with ESF # 2 Annex to the National Response Framework. EB field agents are also trained to support Project Roll Call deployments.[7]

Within each field office, at least one person is trained and designated as the disaster contact for that office's geographic area of responsibility.[8] Field agents who deploy under a FEMA Mission Assignment fall under FEMA's chain-of-command.

C. LINES OF COMMUNICATION

PSHSB maintains secure facilities and manages and operates all secure communications systems (data, facsimile, video, and voice) within the FCC. Minimum Communications requirements for COOP are set out in NCS Directive 3-10 (Minimum Communications).

In order to ensure reliable telecommunications services at FCC headquarters, and the FCC's other essential sites, the FCC enrolled its most critical circuits in the Telecommunications Service Priority (TSP) program.[9] Furthermore, to enable FCC emergency calls to get completed—even when networks are congested—all emergency response staff members at the FCC have Government Emergency Telecommunications Service (GETS) cards;[10] most have Wireless Priority Service (WPS) for their wireless telephones.[11] Some senior managers are equipped with secure terrestrial and satellite telephones (additional phones are being purchased).

In an emergency, FCC management may communicate with staff members inside the FCC's headquarters through various systems.

Also, many FCC staff members have mobile voice and e-mail communication capability during an emergency through the use of FCC issued BlackBerrys and RSA "SecurID" tokens. These tokens permit the user to log into a WebMail version of their FCC e-mail. This allows them to send and receive e-mails and file attachments.

---

[7] A system of radio equipment, computers, and FCC licensing databases that can be brought into a disaster area and activated to determine which radio based systems are operational.

[8] *See* http://www.fcc.gov/pshs/about-us/contacts.html for a list of these contacts.

[9] The TSP authorizes priority provisioning and restoration treatment for certain NS/EP telecommunications services. *See* Part 64 of the FCC's rules, Appendix A and http://www.fcc.gov/pshs/services/priority-services/tsp.html.

[10] GETS is an NCS program that provides priority call queuing over the wireline portion of the PSTN. *See* http://www.fcc.gov/pshs/services/priority-services/gets.html.

[11] The WPS program provides priority call queuing over the wireless portion of the PSTN. *See* Part 64 of the FCC's rules, Appendix B and http://www.fcc.gov/pshs/services/priority-services/wps.html.

SECTION 2: TRAINING AND EXERCISE

2. Describe the FCC's approach to emergency preparedness and continuity training exercises, including:

   - Schedule of training exercises (recent and planned)
   - Description of training exercises and who is involved
   - Results/performance (or underperformance) in most recent exercise(s)
   - "Lessons learned" and corrective action items for each of the exercises and progress to-date on implementing those actions

Emergency COOP Plans will not be effective unless the personnel who are required to carry out the plans are provided training and realistic exercises in which their knowledge of the plans and their roles in the plans can be gauged and improved. Federal Continuity Directives require that key personnel engage in at least one COOP exercise each year, and it is recommended that the agency's exercise coincide with national-level exercises involving many segments of the Federal government.

An essential component of effective emergency planning is that the underlying communications systems are reliable. To ensure the reliability of communications systems for key agencies within the Federal government, FEMA conducts monthly tests of these systems to see how they perform in conjunction with other Federal systems. The FCC passed all recent tests and did so well that FEMA now tests the FCC's communications systems quarterly instead of monthly.

I. TRAINING AND EXERCISES 2005-2010

A. CONTINUITY OF OPERATIONS

As indicated below, the FCC participated in at least one national-level COOP exercise each year since 2005.

April 2005—TOPOFF3 (Top Government Officials) Tabletop Exercise

- Terrorist Attack Scenario
- FCC emergency management officials participated

June 2005—Pinnacle 2005 National-Level COOP Exercise

- Terrorist Attack Scenario
- Senior officials from all Bureaus and Offices participated from the COOP site

June 2006—Forward Challenge 2006 National-Level COOP Exercise

- Natural Disaster Scenario
- FCC emergency management officials participated

May 2007—Pinnacle 2007 National-Level COOP Exercise

- Aftermath of Terrorist Attack Scenario
- Senior officials from all Bureaus and Offices participated from the COOP site

May 2008—Eagle Horizon 2008 National-Level COOP Exercise

- Natural Disaster and Terrorist Attack Scenario
- Senior officials from all Bureaus and Offices participated from the COOP site

June 2009—Eagle Horizon 2009 National-Level COOP Exercise

- Natural Disaster and Terrorist Attack Scenario
- Senior officials and staff members from PSHSB participated from the COOP site

2009-2010—Exercise Plan

The FCC's emergency plans assign specific duties and responsibilities to key individuals. For these plans to be effective, it is essential for all personnel to understand their respective functions during an emergency. With the influx of new leadership, the Chairman ordered an emergency preparedness headquarters exercise for Wednesday, August 19, 2009, to ensure that the FCC is fully versed in procedures for both no-notice emergencies (e.g., earthquakes and terrorist attacks) and anticipated incidents (e.g., hurricanes). In attendance for a three-hour session involving a no-notice event were the Chairman, Commissioners Copps, Clyburn, and Baker, a representative from Commissioner McDowell's Office, and the FCC's Chief of Staff. The Chairman and Commissioners were joined by senior Bureau/Office leadership for a briefing on the FCC's Continuity of Operations (COOP) plan and an exercise that simulated damage to the FCC's main facility.

In the spring of next year, the FCC will participate in a multi-day, interagency COOP exercise. This will require overnight stays at the COOP site for exercise participants. PSHSB will conduct bureau-level and agency-level training at the FCC in anticipation of this event.

B. EMERGENCY RESPONSE

In the aftermath of Hurricane Katrina's impact in the Gulf Coast region, the FCC has been very active in organizing and training FCC and other Federal agency personnel to support Federal communications response and recovery efforts. In addition, the FCC adopted a very proactive approach in assisting its licensees and regulated entities impacted by disasters.

2006—Homestead Air Reserve Base

The first training and exercise session was conducted over the period 20-26 May 2006. This session was held at Homestead Air Reserve Base in Homestead, Florida. The training was jointly conducted with the NCS and its support agencies, with the NCS hosting the training. The focus of the training was an introduction to communications systems along with a simulated hurricane exercise to train personnel on activities within a notional ESF # 2 component of a FEMA-based JFO. In addition, site visits to local communications facilities, Public Safety Answering Points (PSAPs), and emergency operations centers augmented the ESF # 2 training program. Approxi-

mately 100 personnel (either presenters or attendees) participated in the training that was deemed to be very successful.

2007—New Orleans

After the hurricane season of 2006 and following the success of the previous year's training, another–more complicated–training session was conducted in New Orleans, Louisiana, from 19-28 June 2007. Again this was training organized by the FCC and conducted in conjunction with NCS, FEMA, DHS, and the other NCS support agencies, with the NCS hosting the training. Approximately 150 personnel from a number of NCS support agencies participated in the conference. With the moniker "Operation Swift Response," the goal of this communications training and exercise conference was to prepare the ESF # 2 team with the knowledge and skills necessary to ensure effective communications-related coordination, assessment, and restoration by Federal, state, tribal, local agencies and the private sector. In addition to sessions on communications systems, field visits were conducted with parish officials for damage assessments, PSAPs for real-life experience sessions, visits with state emergency management officials, and visits to a vendor emergency equipment demonstration area. In addition, NCS-designated teams deployed to the training conference as part of a hurricane deployment scenario and exercise environment. Once again, the conference was considered a great success by the participants.

2008—Crucible

In addition to national-level exercises, EB field agents participate in training events specific to the regions or states in which they are stationed, such as the wildfire tabletop exercises.

2009—Naval Amphibious Base Coronado

Following the hurricane season of 2008 and with the establishment of an interagency agreement between FEMA's Disaster Emergency Communications (DEC) branch and the FCC, a training session was conducted from 22-25 June 2009 at the Naval Amphibious Base Coronado, California. This training, entitled "Disaster Preparation and Response: Tactical Communications," was intended to prepare FCC personnel to deploy to an incident area and support the FEMA response, particularly with spectrum monitoring equipment and with the abilities to analyze communications outages and determine appropriate remedial actions. This FEMA-sponsored, FCC-organized training was focused on training FCC and FEMA personnel on the roles, missions, and implementation of the Project Roll Call spectrum monitoring equipment. In addition, the training was intended to prepare FCC personnel to support their FEMA counterparts at the regional, state, tribal, and local levels prior to and following an emergency incident. The training included approximately eighty personnel from the FCC (primarily EB personnel) and FEMA emergency response personnel. Once again, the training was well received and the conference was considered a success.

II. RESULTS OF RECENT EXERCISES

A. PINNACLE (MAY 2007)

This exercise was designed to test performance of essential agency functions, interoperable communications, information flow, policy coordination, incident management protocols, protection and stabilization of critical infrastructure, and support of civil authorities and the public safety community. Personnel from the Chairman's Office and all Bureaus and Offices participated in the exercise.

The FCC's performance was rated satisfactory. The FCC took action to address all of the deficiencies that were identified.

B. EAGLE HORIZON (MAY 2008)

The FCC conducted its exercise in coordination with a national-level exercise managed by FEMA. The exercise was designed to test performance of essential agency functions, information flow, policy coordination, incident management protocols, protection and stabilization of critical infrastructure, and support of civil authorities and the public safety community.

The FCC's performance was assessed under the requirements of Federal Continuity Directives. External evaluators observed exercise play and were positioned with players to record information about the performance of the FCC's overarching objectives.

Overall, the FCC received an average rating of 98 percent and a favorable 100 percent rating on all fifty evaluation items designated as critical. This was an exceptionally good score. The evaluation considered the FCC's COOP Plan, Devolution Plan, IT resources, and operational coordination and performance. All rating elements required complete documentation. The FCC's ratings signify that it had no significant deficiencies with the respective continuity elements and no significant compliance or implementation concerns.

SECTION 3: REAL-WORLD INCIDENTS

3. Describe any real-world incidents over the past 5 years that required the FCC to initiate its emergency plan (including false alarms).

   - What was the incident?
   - What was the agency's response?
   - How did the agency perform?
   - What improvements were identified as a result of each incident or problems with the FCC's performance and what is the progress towards implementing the improvements or corrective action?

In the last five years, there have been no real-world incidents that have required the FCC to initiate its COOP plan. However, between 2005 and the present, the FCC implemented emergency response procedures in connection with major hurricanes, as well as other weather related events and NSSEs. The nature of the FCC's response varied with the scope and magnitude of each event. In some instances, the FCC activated emergency management teams while for others it deployed personnel for direct and indirect supporting roles. A summary of the major events of the last five years appears below.

I. FCC EMERGENCY RESPONSE ACTIVITIES IN 2005

A. HURRICANES KATRINA AND RITA

Hurricane Katrina marked the first significant deployment of FCC staff in a disaster recovery role. The FCC deployed senior staff with technical and policy expertise to the NCS's National Coordinating Center for Telecommunications (NCC). At FCC headquarters, an emergency management team comprising staff members from the Chairman's Office and all Bureaus and Offices operated 24/7 to support the relief efforts.

One of the first requirements identified by the FCC team was the ability to obtain consistent, comprehensive, and up-to-date reports on the operational status of essential communications systems and services in the affected area. This information would enable the FCC to advise leadership on setting priorities regarding which communications systems to restore first and how best to apply the resources required. As a result, beginning within twenty-four hours of Hurricane Katrina's landfall, the FCC worked closely with the communications sector to develop *ad hoc* outage reporting mechanisms and created a computerized system for compiling and analyzing the outage and restoration data. The FCC used the data to prepare daily reports for the FEMA, NCS, OSTP, and other agencies engaged in the recovery process. The FCC developed and refined this data collection and reporting process during the first weeks after the disaster and provided daily reports for several months that tracked the restoration of communications systems.

In late September 2005, when Hurricane Rita also threatened the Gulf Coast region, NCS requested that FCC personnel be deployed to FEMA's JFOs in Baton Rouge, Louisiana and Austin, Texas. After Hurricane Rita, additional FCC personnel were assigned to the JFO in Baton Rouge.

FCC personnel also deployed to the New Orleans Area Field Office and each of the affected parishes to perform assessments and analysis of infrastructure damage and to work with state and local officials and industry. The final team members departed in December 2005.

During the 2005 hurricane season, the FCC took a number of steps to cut red tape to facilitate communications restoration. For example, in the aftermath of Hurricane Katrina, the FCC established an expedited process for communications providers in the affected areas to obtain STAs to construct and operate new temporary facilities where existing facilities had been requested. The FCC granted at least ninety STA requests and more than 100 temporary frequency authorizations for emergency workers, organizations, and companies to provide wireless and broadcast service in the affected areas and shelters. In most cases, the requests were granted within four hours; all requests were approved within twenty-four hours.

Although the FCC received high marks in comparison to many other Federal agencies for its efforts in response to hurricanes Katrina, Rita, and Wilma, experience also revealed significant vulnerabilities in planning and preparation for a catastrophic event affecting the communications sector.[12] Four major areas for improvement were identified:

B. AREAS FOR IMPROVEMENT

Develop a user-friendly operational data collection system that enables each major industry segment (e.g., wireless, wireline, broadcast, and cable) to report status and outage data, which the FCC can then use to analyze and prepare situational reports.

> **Solution**—The FCC, working with the NCS, developed DIRS in 2006-2007. This system was first used in 2008. An improved version is in place today.

Revise and update out-of-date standard operating procedures (SOPs) for ESF # 2 to reflect emergency needs and the authorities, skills, and responsibilities of the ESF # 2 support agencies.

> **Solution**—SOPs were re-written in 2006 and have been updated periodically; today they serve as key source guides for organization planning, structure, and processes.

Develop and fund training programs for Federal emergency communications managers and responders.

> **Solution**—The FCC, in coordination with the NCS, organized and implemented a week-long emergency training and exercise conference in the summer of 2006. The curriculum included training on technical, academic, and emergency issues. Since then, approximately 150 emergency communications responders have received technical, academic and exercise play training in FEMA processes, telecommunications, and land mobile radio (LMR) technologies. Funding for this type of training is still an issue.

Develop a system for rapidly determining the operational status of critical radio-based communications systems in the disaster area.

[12] *See infra* Section 8.

Solution—In 2007 the FCC developed Project Roll Call, a system of radio equipment, computers, and FCC licensing databases that can be brought into a disaster area and activated to determine which radio based systems are operational. The Project Roll Call units provide information on broadcast, commercial wireless, and public safety LMR systems. The systems provide rapid reporting that enables Federal emergency managers to determine which radio-based systems must be restored on a priority basis. To date, with FEMA's financial support, the FCC has assembled Project Roll Call units for disaster response.

II. FCC EMERGENCY RESPONSE ACTIVITIES IN 2006

There were no storms or other disasters during 2006 that required FCC involvement in the response.

III. FCC EMERGENCY RESPONSE ACTIVITIES IN 2007

ESF # 2 was restructured with FEMA becoming a co-primary ESF # 2 agency with responsibility for coordinating the Federal tactical communications response, which includes command-and-control communications for Federal, state, tribal, and local government entities, public safety communications (e.g., police, fire, emergency medical services, hospitals, and 9-1-1 call centers). FEMA also provided the funding for Project Roll Call.

Two tornadoes, one in central Florida, and the other in Greenburg, Kansas, elicited FCC responses. For the former, an EB field agent from the Tampa Field Office conducted a damage assessment, and PSHSB staff members responded to a cable provider's complaint that work crews were indiscriminately cutting its cables on damaged utility poles without coordinating with cable owners. Coordination was accomplished after PSHSB contacted Florida's Division of Emergency Management. With respect to Greenburg, an EB field agent from the Kansas City Field Office coordinated the issuance of STAs in order for Traveler's Information Stations to carry emergency information.

The success of the 2006 FCC-led ESF # 2 training generated a request for the FCC to conduct a full-scale ten-day ESF # 2 training in New Orleans for 2007, which the NCS hosted. Fifty persons from EB and PSHSB participated in the training, which included technical classroom lectures, visits to sites devastated by Hurricane Katrina, a session at Louisiana's Emergency Operations Center, a walk-through of the Baton Rouge JFO, and a hurricane response exercise.

In 2007, DIRS was launched. This voluntary system allowed for a more rapid identification of outages in the disaster area.

IV. FCC EMERGENCY RESPONSE ACTIVITIES IN 2008

In 2008, the Midwest Floods, hurricanes Dolly, Hanna, Gustav and Ike, and Tropical Storms Edouard and Fay tested the enacted changes to the FCC mission, PSHSB's Incident Management Team, and the new ESF # 2 structure.

A. MIDWEST FLOODS

In June 2008, severe flooding took place in Illinois, Indiana, Iowa, Michigan, Minnesota, Missouri, and Wisconsin. ESF # 2 was activated for the Iowa flooding and an EB field agent (Kansas City field office) drove a direction-finding vehicle to Grand Rapids, Iowa to assist FEMA in identifying interference to one of its satellite assets.

For PSHSB Operations Center staff members, response activities included weather monitoring, weather and flood analysis, and situation reporting. Operations Center staff members became familiar with flood stages, river crests, levee locations, and flood plain models, and used NCC Sea, Lake, and Overland Surge from Hurricane (SLOSH) models to provide situational awareness of the flood damage. Staff consolidated key information on communications infrastructure damage and prepared situational awareness reports for senior FCC leadership. The Operations Center also received and acted on after hours STA requests. EB field agents deployed to assist in the response efforts for these events.

B. HURRICANE SEASON

A PSHSB staff member was deployed with FEMA's national IMAT to the Florida emergency operations center in Tallahassee, Florida for Tropical Storm Fay in August 2008. The PSHSB staff member conducted a damage assessment of Broward County, but this event did not result in formal ESF # 2 deployment.

The IMT, primarily composed of PSHSB personnel, but also staffed and supported by representatives from other Bureaus and Offices was activated. The IMT managed and coordinated the FCC's response and focused on outreach and assistance to the FCC's licensees and regulated entities.

For Hurricanes Gustav and Ike, the FCC deployed two teams pursuant to FEMA-generated mission assignments: one three-person team for Project Roll Call operations (as part of the IMAT) and another six-person team to provide support to a FEMA JFO. The Project Roll Call team put in a total of 6,910 miles on the road. The team assigned to the FEMA JFO also included one person from NTIA.

For Hurricanes Gustav and Ike, PSHSB's Operations Center conducted sweeps of AM broadcast stations through the FCC's High Frequency Direction Finding Center (HFDFC) and provided twice-daily situation briefs to FCC leadership. PSHSB personnel reached out to hundreds of FCC licensees and regulated entities through telephone calls and other means before and after storm landfall and to PSAPs throughout Louisiana and Texas, as well as to hospitals. Operations Center staff members also continued to monitor, receive, and approve STA requests received outside of normal FCC business hours.

PSHSB, in consultation with the NCS, also activated DIRS as the storms approached. DIRS provided critical communications infrastructure data that improved situational awareness and assisted in the recovery efforts.

C. POLITICAL CONVENTIONS

The HFDFC and EB deployed personnel to the Republican and Democratic National Conventions to support the Principal Federal Official and Federal departments and agencies in the monitoring, tracking, and identification of interference for these events. This was the first time in recent memory that HFDFC specialists participated in a field deployment. In one instance, HFDFC personnel were able to find a foreign-based wireless microphone that was operating in an unauthorized spectrum. Such successes highlight the need for continued support for the systems and software used by the HFDFC both in mobile and static national and public safety activities.

D. ACCOMPLISHMENTS AND AREAS FOR IMPROVEMENT

Accomplishments during the 2008 Hurricane Season included:

- Initial use of DIRS to collect information on the operational status of communications systems in a disaster area.
- Development and implementation of an IMT.
- Initial use of Project Roll Call to determine the operational status of radio communications systems in a disaster area.
- Development and distribution of daily operational situation briefs, charts, and maps describing situation awareness and network status.
- Outreach by PSHSB personnel to public safety entities.
- Outreach by other Bureau personnel to FCC licensees.
- On-the-ground field support of ESF # 2 mission assignments.
- Strengthening of the FCC's relationship with FEMA, both at the FEMA headquarters and its regional levels, especially with regard to development and deployment of Project Roll Call, participation on the FEMA IMATs, and direct support to FEMA at the JFO.

Several areas for improvement were also identified:

- Data sets were not readily available or on common platforms that allowed analysis or integration into daily reports.
- The skill sets needed for headquarters staff as well as those in the field were not adequately identified.
- Processes that proved effective must be documented and integrated into the IMT SOPs for use in future incidents.
- Additional human capital resources are needed—work was conducted by a limited number of staff at FCC headquarters and from EB's field offices. Many of these emergency team members had to work long hours, including shifts of more than twelve hours per day, in order to accomplish all of the essential tasks.
- The formatting, timing, tracking and progress notifications of system operations and out-

age situation reports and situation briefs should be re-examined.

Areas that require additional training include:

- Robert T. Stafford Act interpretation and training.[13]
- Organizational roles and responsibilities.
- Outreach requirements.
- Analysis and plotting of essential communications assets.
- Liaison reporting and tracking of contacts and need requests workflow.
- Pre-scripted public notices and outreach scripts.
- FCC roles and responsibilities as part of the overall Federal response.
- Cross training the staff.
- FCC field staff training as Project Roll Call operators.
- Using DIRS to collect status information.
- Interpretation of DIRS reports.

[13] Robert T. Stafford Disaster Relief and Emergency Assistance Act, PL 100-707, signed into law November 23, 1988; amended the Disaster Relief Act of 1974, PL 93-288. This Act constitutes the statutory authority for most Federal disaster response activities especially as they pertain to FEMA and its programs.

SECTION 4: COMMUNICATIONS FAILURE PREVENTION

4. Describe ongoing proactive efforts to prevent communications failures in large-scale emergencies:

   - Monitoring the nation's telecommunications infrastructure
   - Assessment of infrastructure survivability
   - Any known weak spots of special concern

The FCC has several programs and systems in place to help prevent communications failures in large-scale emergencies.

I. NETWORK OUTAGE REPORTING SYSTEM (NORS) AND ANALYSIS

Part 4 of the FCC's rules requires communications providers, including wireline, wireless, paging, cable, satellite, and Signaling System 7 service providers, to report communications disruptions to two-way voice and/or data communications that meet certain thresholds specified in those rules. When a major outage occurs that triggers the reporting thresholds, affected communications providers file outage reports through the Network Outage Reporting Systems (NORS), a secure web-based filing system. NORS uses an electronic template to promote ease of reporting and encryption technology to ensure the security of the information filed. NORS is a fault-tolerant, redundant system that has a resilient IT architecture at FCC headquarters and a failover mechanism to the FCC's COOP site. PSHSB's Communications Systems Analysis Division (CSAD) maintains NORS. NORS outage reports are presumed to be confidential, however, NCS has access to NORS and is able to review the reports filed.

Part 4 requires communications providers to file an initial outage report within two hours of discovering a reportable outage. The provider must file an updated report on the outage within three days and a detailed final report within thirty days. NORS is an important vehicle for the FCC and NCS to obtain an early assessment of the impact on communications from major emergencies like power outages, ice storms, tornadoes, and earthquakes. This information is used by the FCC and NCS to decide what type of emergency response is necessary, including whether DIRS should be activated for the emergency. PSHSB also reviews the outage reports submitted through NORS every weekday morning and assigns significant reports for follow-up action.

The outage information filed in NORS also provides valuable data for analyzing network vulnerabilities, improving network reliability, and preventing future communications failures. PSHSB analyzes the outage reports using statistical methods to discern any outage trends and patterns of outages both for individual carriers and for the industry as a whole (often disaggregated by platform delivery system, *i.e.*, wireline, wireless). PSHSB is in regular contact with individual carriers to discuss any troubling trends that might be detected, such as an increase in the number of DS3 outages or upswings in the loss of ANI/ALI (associated name and location information) links in connection with the operation of E-911 services. Review and analysis of NORS data enables PSHSB to see major trends in network reliability that are invisible to individual communi-

cations providers. NORS data has revealed a number of network reliability issues and systemic weaknesses in the communications infrastructure that have been shared with industry bodies for further study and resolution.

II. DISASTER INFORMATION REPORTING SYSTEM (DIRS)

The Disaster Information Reporting System is the voluntary web-based system through which the FCC collects daily operational status and restoration information during major disasters and subsequent recovery efforts from communications providers, including wireless, wireline, broadcast, and cable providers. DIRS information allows the FCC and other ESF # 2 support agencies to track the status of the communications sector's operations and restoration efforts in the aftermath of a large-scale emergency and to determine outstanding needs (e.g., generators, fuel, access, security).

III. TRACKING THE RESILIENCY OF 911 AND E911 SYSTEMS

Section 12.3 of the FCC's rules requires that certain LECs, commercial mobile radio service (CMRS) providers, and interconnected Voice over Internet Protocol (VoIP) service providers analyze their 911 and E911 networks and/or systems and provide a detailed report to the FCC on the redundancy, resiliency, and reliability of those networks and/or systems. Pursuant to delegated authority, PSHSB determines the specific data required and collects that information. Where relevant, these reports are to include steps that service providers intend to take to ensure diversity and dependability in the network and/or system, including any plans for migration to a next generation IP-based E911 platform. The deadline for submission of this information passed on February 6, 2009; PSHSB is currently preparing an analysis of this data that evaluates the resiliency of the 911 and E911 systems.

IV. FEDERAL ADVISORY COMMITTEE ACTIVITIES

The FCC has used Federal Advisory Committees to address issues relating to the security, reliability, and interoperability of communications systems. Two advisory committees, the Network Reliability and Interoperability Council (NRIC) and the Media Security and Reliability Council (MSRC), were previously established to develop best practices for ensuring reliability and resiliency in telecommunications networks and media systems, respectively. In 2007, the FCC terminated NRIC and MSRC and established a new advisory committee, the Communications Security, Reliability, and Interoperability Council (CSRIC), to replace them. Although the CSRIC was initially chartered in 2007, no members were selected at that time and the committee did not convene before its initial charter expired. The FCC subsequently renewed the CSRIC Charter in March 2009, and PSHSB solicited nominations for membership. PSHSB anticipates that CSRIC members will be selected and CSRIC will convene later this year.

V. ASSESSMENT OF INFRASTRUCTURE SURVIVABILITY

A. COMMERCIAL COMMUNICATIONS SURVIVABILITY

All the activities described above to monitor the telecommunications infrastructure also include assessments of infrastructure survivability. For example, NORS collects information on redundant transport facilities that have lost the diverse connection. Such conditions, while survivable, are vulnerable to large-scale failure until diversity is restored. When NORS information revealed this to be a problem area, PSHSB staff worked with industry to reduce the number of these events, resulting in dramatic improvements.

B. PUBLIC SAFETY COMMUNICATIONS SURVIVABILITY

PSHSB periodically conducts technical case studies of how specific disasters or incidents have affected the performance of emergency communications systems. Past case studies include a study of the performance of emergency communications following the 2007 collapse of the Interstate 35 Bridge in Minneapolis, Minnesota, and a vulnerability assessment of the Nation's critical communications and information systems infrastructure and a technical feasibility analysis of a back-up emergency communications system, which was prepared for Congress as required by the 9/11 Commission Act.[14]

VI. KNOWN WEAK SPOTS OF SPECIAL CONCERN

A. IP-BASED COMMUNICATIONS NETWORKS AND TELECOMMUNICATIONS RELAY SERVICE (TRS) FACILITIES

The evolution of communication technologies from circuit-switched to packet-switched capability has led to the emergence of communication services that utilize IP network infrastructure, such as interconnected VoIP and Internet-based TRS. However, the FCC's network outage reporting rules do not apply to IP-based services, but only to traditional telecommunications services. Thus, its ability to collect information, analyze, and remedy disruptions to communications is significantly more limited with respect to IP-based communications networks and services provided by Internet Service Providers (ISPs).

B. BACKUP POWER

Backup power (e.g., batteries, generators) is essential to the redundancy and resiliency of the communications infrastructure in the event of a power outage. On June 8, 2007, following a recommendation by the FCC's Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks ("Katrina Panel"), the FCC adopted a rule that required certain wireline and wireless communications providers to maintain backup power capability at their facilities. In a subsequent Order on Reconsideration, the FCC revised this rule to address concerns about the backup power requirements raised by wireless communications providers. The rule, however, has been stayed by the U.S. Court of Appeals for the District of Columbia Circuit based on a wireless industry appeal, and the Office of Management and Budget (OMB) has rejected the

[14] *See* http://www.fcc.gov/pshs/docs/fcc9-11report.pdf.

associated information collection. In December 2008, the FCC's Office of General Counsel requested that the Court dismiss the pending appeal as moot because the FCC does not intend to implement the rule and instead plans to issue a new Notice of Proposed Rule Making (NPRM) to develop a revised rule. To date, the Court has not acted on the FCC's request for dismissal and the FCC has not issued a new NPRM.

C. EMERGENCY ALERT SYSTEM

The Emergency Alert System (EAS) is a nationwide emergency alerting mechanism pursuant to which broadcasters, cable and wireless cable television systems, and other service providers identified by the FCC must provide communications capability to the President to address the nation in a national emergency. EAS also is available at the state and local level to enable EAS participants, on a voluntary basis, to transmit local or state emergency information, such as severe weather alerts and child abduction alerts ("Amber Alerts"). The FCC, FEMA, and the National Oceanic and Atmospheric Administration (NOAA) implement EAS at the Federal level.

Concerns have been raised regarding the frequency and scope of EAS testing. The three Federal partners should review the testing regime to see where improvement can be made.

SECTION 5: CYBER ATTACK RESPONSE

5. Describe any efforts of the FCC to detect or respond to a cyber attack:

- Proactive steps taken with the carriers
- Agency response plans

Cyber attacks have the potential to harm communications systems and providers that the FCC regulates, as well as the FCC's own IT systems.[15] With respect to the FCC's own IT technology, OMD has a variety of tools and methods for detecting and responding to cyber attacks on FCC systems. The FCC, however, is much more limited in its ability to detect independently, monitor, and analyze cyber attacks outside the FCC. This is because the FCC's existing tools for monitoring and enhancing the resiliency of communications networks are focused on physical threats to the traditional circuit-switched telecommunications infrastructure, and do not extend to IP-enabled networks. In addition, certain types of cyber attacks may not be detected because they are directed at specific network users but do not cause harm to the networks themselves. Despite these limitations, the FCC has engaged in collaborative efforts with industry and other government agencies to enhance its awareness and ability to respond to cyber attacks. PSHSB believes, however, that the FCC should consider significant expansion of its cyber security role.

I. DETECTION

The FCC currently has no mechanism to collect—on a mandatory basis—data on the functioning of IP-based networks to monitor, detect, and analyze cyber attacks. It relies instead on a variety of U.S. Government and open sources of data.

A. PROACTIVE EFFORTS WITH TELECOMMUNICATIONS PROVIDERS

Part 4 NORS Although Part 4 is concerned with disruptions to the communications physical infrastructure, the Presidential Cyberspace Policy Review acknowledges that such outages may impair IP-based communications. For example, a single large transport systems outage can affect traffic running on a variety of network platforms (e.g., traditional Public Switched Telephone Network, Next Generation Networks, and Ethernet). The FCC's existing Part 4 rules explicitly exclude VoIP. The existing Part 4 rules regarding transport outages simply require that notice be provided when traffic flows of certain communications providers have been impaired, not what

[15] Because cyber attacks can be perpetrated upon the physical communications infrastructure as well as its virtual counterpart, for purposes of this review, cyber attacks are defined in the comprehensive manner adopted by the Presidential Cyberspace Policy Review. The Presidential Cyberspace Policy Review adopted the definition of cyberspace set forth in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), which defines cyberspace as:

> [T]he interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.

kinds of traffic flows were affected by the disruption or the networking protocols involved. IP-enabled technology introduces a vertical dimension to communications, including higher layer data protocols, services, and applications. Communications reliability and performance at these higher layers is neither exclusively, nor even predominantly, dependent on happenings lower down in the protocol stack.

DIRS DIRS, like NORS, currently collects information on damage to physical infrastructure (either willful or due to natural disasters). Damage of this type is relevant to cyber security to the extent that vulnerabilities are exploited physically, though that is not the typical attack mechanism. More often, cyber attacks occur at the logical layer. Today, DIRS does not provide independent information at this layer.

B. PROACTIVE EFFORTS WITH ISPs AND THE GOVERNMENT

ISPs The FCC has authority to regulate entities that provide communication services via the Internet, and that authority might include the regulation of the underlying infrastructure used to provide those services. If an IP-based service is a "telecommunications service" within the meaning of 47 U.S.C. § 153(46), the FCC has authority to regulate a provider of that service under Title II of the Communications Act. If an IP-based service is an "information service" within the meaning of 47 U.S.C. § 153(20), the FCC may have authority to regulate a provider of that service pursuant to Title I ancillary jurisdiction. However, the FCC's Title I ancillary jurisdiction is not limitless and the extent of the FCC's authority to regulate information services pursuant to Title I ancillary jurisdiction has not been defined clearly.

Today, the FCC does not require ISPs to file outage information akin to that received from traditional communications providers under the Part 4 rules. The FCC does receive information on the general health of cyberspace from DHS, other governmental entities, and the private sector.

DHS Cyber information from the National Cyber Security Division of DHS flows into the FCC's Operations Center, OMD's Information Technology Center, and directly to CSAD staff. The FCC also has access to US-CERT resources, including US-CERT Daily briefings on cyber trends and incidents against government and non-government computers.

The FCC regularly monitors DHS's Internet Health Services, which provides real-time and forensic information on global Internet routing maps and their changes, routing failures, instabilities, and security incidents. These tools also organize IP networks into critical infrastructure sectors. This provides, for example, the ability to identify outages cutting off Internet access for cable modem and digital subscriber line (DSL) ISP service to a fairly local geographic level. Finally, the FCC monitors network operator discussion lists, where cyber attacks are often reported and compared. The effects of significant incidents affecting ISPs are routinely matched against related NORS outage reports received from carriers.

Other Government Information The FCC participates in meetings of the NCC, which facilitates an exchange among government and industry participants regarding vulnerability, threat, intrusion, and anomaly information affecting the telecommunications infrastructure. The FCC also serves on joint Industry/Government Sector Specific Planning efforts, which include a focus on

IT vulnerabilities and responses. The FCC conducts internal studies and briefings on cyber issues, for example on cyber security issues in hybrid telecom systems.

C. RECOMMENDATIONS FOR IMPROVEMENT

Expansion of NORS The FCC could consider expansion of Part 4 Outage Reporting Rules to include broadband ISPs. PSHSB notes that this would require consideration of the extent to which the FCC has jurisdiction to regulate the network management practices of ISPs and other "information service providers," including the filing of reports.

Real-time monitoring of IP networks There are no rules that provide the FCC with independent monitoring of IP-based networks. The FCC currently depends on U.S. Government and open source data. While useful, these sources lack the detail necessary to give the FCC a sophisticated, objective understanding of the status of IP-based networks.

ISPs have access to this data for their own networks, using it to manage their networks and to give certain customers greater visibility about network status. For example, one provider's cyber security platform monitors all flows at network edges (peering points, access nodes, etc.), has flow detectors on the internal network that can detect distributed denial-of-service (DDoS) attacks, and monitors all alarms and audit logs for all appliances within the network. Such data would permit the FCC to make data-driven conclusions about the real-time and long-term health of cyberspace.

Expansion of DIRS One major ISP informally expressed its interest in sharing its internal network monitoring of cyber attacks with the FCC and other ISPs, but has requested that the FCC act as a trusted monitor to ensure that any sharing would be reciprocated and structured in such a fashion that ISP proprietary information would remain confidential.[16] Such a system could be set up as a Broadband analog of DIRS. As discussed above, DIRS is voluntary, thus ISP and other broadband provider participation in a Broadband-based DIRS would avoid the jurisdictional issues associated with a Broadband-based NORS or other mandatory obligations.

II. RESPONSE

Cyber security Best Practices—NRIC One means by which the FCC has previously sought to address cyber security has been through the NRIC, a former Federal Advisory Committee composed of private sector representatives that cataloged proven operational best practices for carrying out network engineering, monitoring, and maintenance functions. The NRIC has been superseded by the CSRIC, but NRIC cyber security best practices remain available on PSHSB's website and are increasingly relevant. [17] NRIC's work on cyber security was conducted by leading network operators from the communications sector and resulted in over 200 new best practices to help service providers secure their networks against accidental events and criminal activities.

[16] Another avenue for consideration is the role of unlicensed operators, such as Wireless ISPs or WISPs, and the information that they could provide.

[17] Available via the FCC's website, https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm.

NRIC cyber security best practices can be categorized into four basic areas: (1) updating software; (2) secure equipment management; (3) intrusion prevention and detection; and (4) intrusion analysis and response.

Best Practices Outreach While many of the largest communications sector participants were members of NRIC, and will likely be members of CSRIC as well, there are other entities that have not been involved in the process. The FCC has turned to outreach and education to expand awareness and encourage implementation of NRIC best practices, including those aimed at improving cyber security. Venues for these educational seminars include state and national telecommunications associations, with a primary emphasis on reaching small independent service providers. Cyber security best practices are broadly applicable to both the closed IP networks that communications providers use to manage their networks and the publicly-accessible IP networks operated by ISPs, and thus outreach has also been extended to ISP operator forums.

Rechartering of CSRIC The FCC recently re-chartered the CSRIC, a Federal Advisory Committee that succeeds the NRIC and MSRC and is tasked with developing recommendations for best practices and actions the FCC can take to enhance the operability, security, and reliability of communications infrastructure. CSRIC's charter directs the Council to develop new best practices to "[t]ake into account new and advanced technologies including broadband and IP-based technologies."

Participation in Public-Private Partnerships PSHSB staff members regularly attend meetings of the President's National Security Telecommunications Advisory Committee (NSTAC) and its constituent working groups and task forces as part of the FCC's ongoing commitment to secure telecommunications networks. As part of this collaboration, FCC staff members participated in the NSTAC's Cybersecurity Collaboration Task Force, established in November 2008, to explore the feasibility of creating a joint 24/7 public-private operational capability that would improve the Nation's ability to detect, prevent, mitigate, and respond to significant cyber events. FCC staff members also are participating in the Identity Issues Task Force, which recently produced a report with recommendations on secure Identity Management.

The FCC is monitoring and analyzing work taking place in study groups and other fora of the International Telecommunications Union (the international standards-setting body for telecommunications) pertaining to cyber security. This work is conducted under the leadership of the Department of State.

Incident Analyses The FCC generates internal analysis and briefing papers of newsworthy cyber events for which the FCC may be expected to be knowledgeable. FCC staff members have also undertaken forward-looking studies of cyber security issues.

FCC Response to Events Where events are associated with physical infrastructure, the FCC has a series of responses which it is prepared to provide to affected industry members. For example, the FCC may grant STAs to reconstruct infrastructure or to operate in an alternative mode while infrastructure is being replaced. However, where an attack is purely cyber-based, such as denial-of-service (DoS) attacks or attacks on the Internet routing infrastructure, the FCC does not currently have procedures regarding response.

SECTION 6: PANDEMIC EMERGENCY RESPONSE

6. Describe any efforts of the FCC to prepare for or respond to a public health emergency, such as a pandemic:

   - Steps to keep the agency operational if health risks cause the offices to close
   - Steps to keep the national communications infrastructure operational

Over the past year, extensive work has been completed on pandemic planning in response to recent White House directives on pandemic and the H1N1 outbreak. OMD and PSHSB are working together to incorporate the new guidelines into a revised Pandemic Response Plan, which is currently in draft form and will be included as a supplement to the COOP Plan.

Unlike other catastrophes, a pandemic generally will not result in physical damage to the FCC's facilities and assets, but could threaten the availability of the FCC's human resources at the workplace (including contractors as well as FCC staff) for extended periods of time. Thus, preparation for a pandemic requires the FCC to consider how to accomplish its mission when its staff must work from remote locations and, often, with mobile equipment.

DHS has primary responsibility within the Federal government to manage the domestic impact of a pandemic, with assistance from the Department of Health and Human Services and the Centers for Disease Control (CDC). The FCC will follow guidance articulated by the CDC during a pandemic. The PSHSB Chief is designated as the FCC's Pandemic Coordinator.

In revising the Pandemic Response Plan, PSHSB is working closely with OMD and representatives from each Bureau and Office to address four areas of concern during a pandemic: human capital; IT resources; health and safety; and internal and external communications. The Bureaus and Offices have identified lines of succession or subject matter experts that can perform their essential functions, and have also identified the functions that can be accomplished remotely through telework and which, due to current equipment capabilities, must be performed from an FCC facility. PSHSB, in conjunction with Bureau and Office representatives, maintains a list of emergency response personnel with contact information.

PSHSB maintains Internet pages with extensive information about pandemics. *See* http://www.fcc.gov/pshs/emergency-information/pandemics.html.

I. HUMAN CAPITAL ISSUES

During a pandemic, the need for social distancing is imperative.[18] Telework and other alternate work arrangements, e.g., staggered working hours, flex-time, etc., may need to be utilized to the fullest extent.

[18] Reduction of the frequency, proximity, and duration of contact between persons to reduce the chances of spreading the disease.

The FCC relies on Office of Personnel Management (OPM) guidance regarding sick leave, overtime pay, and telework policies.

The FCC plans to rely on existing contractors and support services to continue its operations during a pandemic. Additional and alternate service-level agreements with existing contractors and other third-party service providers may be utilized to support the performance of the FCC's mission.

II. HEALTH AND SAFETY

In the event of a pandemic, OMD will provide information to all employees on illness prevention, the importance of proper hygiene, stress management, and individual and family emergency planning. OMD will also provide personal protective equipment (e.g., face masks, disposable gloves, waterless hand cleaners, etc.) to essential personnel to minimize the spread of infection. Currently, the FCC has 25,000 N-95 masks. Supplies have been distributed to all field offices in addition to the stock at FCC headquarters. The FCC also possesses 2,300 "Go Kits" at headquarters and the field to cover staff if needed for shelter-in-place.

III. COMMUNICATIONS SECTOR PLANNING

PSHSB, along with the other Bureaus and Offices, met with the major telecommunications service providers and trade associations to discuss their pandemic planning. At these meetings, most of the major telecommunications providers provided information on pandemic plans they have in place that provide for potential absenteeism by employees and the potential effects on communications due to increased volume and traffic patterns. However, meetings with trade associations suggest that levels of pandemic preparedness vary considerably among the communications sector, and that some providers may be less well-prepared than others.

In addition to these actions, PSHSB held a Pandemic Planning Summit on September 18, 2008. The video of the summit is available on the PSHSB website.
See http://www.fcc.gov/pshs/summits/.

SECTION 7: EMERGENCY PREPAREDNESS GAPS

7. What risks and gaps in capabilities for emergency preparedness exist (e.g., personnel, budget, monetary, procedures, training/exercises, legal policy, other)?

This review has examined in depth the FCC's preparedness for a major emergency, whether that emergency affects any section of the U.S. or the FCC itself, and the FCC's capability to respond to the emergency effectively, efficiently, and speedily. While the overall results of the review are positive, the review identified actions that can be taken by the FCC to improve its readiness posture and its response capability. Some actions can be taken and completed immediately. Others will take some planning, time, and resources to complete.

It is recommended that the following list form the basis of an FCC-wide action list for implementation, with PSHSB responsible to the Chairman for monitoring and periodically reporting each item's progress through completion.

1. EMERGENCY READINESS TRAINING, EXERCISES, AND PROCEDURES

The FCC's emergency plans assign specific duties and responsibilities to key individuals. For these plans to be effective, it is essential for all personnel to understand their respective functions during an emergency. The arrival of new leadership at the FCC in the past few months increases the importance of making sure that the relevant individuals are familiar with and ready to perform their functions in an emergency.

Solution—The Chairman has directed that training and exercise be an integral part of the FCC's Continuity of Operations program. On Wednesday, August 19, 2009, the Chairman ordered an emergency preparedness headquarters exercise to ensure that the FCC is fully versed in procedures for both no-notice emergencies (e.g., earthquakes and terrorist attacks) and anticipated incidents (e.g., hurricanes). In attendance for a three-hour session involving a no-notice event were the Chairman, Commissioners Copps, Clyburn, and Baker, a representative from Commissioner McDowell's Office, and the FCC's Chief of Staff. The Chairman and Commissioners were joined by senior Bureau/Office leadership for a briefing on the FCC's Continuity of Operations (COOP) plan and an exercise that simulated damage to the FCC's main facility.

PSHSB will continue to develop additional training and exercises to prepare all FCC employees—leadership and staff members alike—for emergency situations.

2. EMERGENCY OPERATIONS OUTREACH SPECIALIST

In prior deployments of FCC emergency communications responders, PSHSB has found that, unless the FCC had established close working relationships with the state, tribal, and local emergency response community in an area prior to a disaster, it generally experienced delays and

other impediments to its initial emergency response instead of a timely, effective, and efficient response.

PSHSB has tried to reconcile this by having FCC headquarters personnel travel to a number of areas around the Nation to conduct outreach, emergency planning, and coordination. This activity is subject to the constraints of PSHSB's limited travel budget.

Solution—The Chairman will deploy a new Emergency Operations Outreach Specialist under a pilot project to the Gulf States region. It is crucially important to establish working relationships with and the support of public safety officials before incidents occur. The coordinator will have primary responsibility for building these relationships, providing pre-incident support and then, in emergencies, would become the main FCC first responder in the disaster area, performing emergency response duties with alacrity. Additionally, the coordinator will perform duties under the FCC's spectrum-monitoring Project Roll Call.

Depending on the success of this pilot project, the Chairman will consider establishing up to three more positions in various areas in the country over the course of the next three to six months.

3. ENHANCED COMMUNICATIONS AND COOPERATION WITH FEMA

The Chairman and FEMA Administrator Craig Fugate have already been in contact and established a good working relationship. Given the value of this partnership, the Chairman has designated Jamie Barnett, PSHSB Chief, to serve as the FCC liaison to Administrator Fugate's team. The Chairman and Administrator Fugate have agreed to establish a high-level working group to find proactively ways to improve effectiveness and efficiency. This effort will include alerting systems and also credentialing private sector communications crews to provide them with ready access to disaster areas. Several high level meetings have occurred which presage a new era of cooperation and teamwork between FEMA and the FCC. In addition, the FCC and FEMA will continue to work together on Project Roll Call and will examine legislative proposals to improve the Stafford Act.

A persistent problem with emergency communications response is that private industry equipment restoration crews are often not allowed into a disaster area, and, therefore, cannot quickly restore vital communications systems for emergency responders or the public. This seriously impedes communications within the disaster area and hampers the overall disaster response. Providing credentials to private sector communications crews to afford them access to disaster areas would appear to be the solution. The FCC has worked with FEMA, which has primary responsibility for this issue within the Federal government. The challenge, however, is much larger, as local authorities generally control access to disaster areas.

Certain provisions of the Stafford Act limit the FCC's ability—through FEMA—to help for-profit critical infrastructure entities in a disaster situation. This has resulted in the inability of Federal emergency personnel to assist, for example, broadcasters that provide essential emergency information to at-risk population segments such as non-English speakers.

Solutions—The FCC will continue to work with FEMA and NCS on credentialing issues, especially through Federal, state, tribal, and local joint working groups. These working groups contain many key state, tribal, and local officials who have authority to accept credentials held by private sector crews.

The FCC will work with DHS to propose legislative changes to the Stafford Act to allow certain types of emergency assistance to for-profit entities that control critical communications infrastructure.

Several high level meetings have occurred already which presage a new level of cooperation and teamwork between FEMA and the FCC.

4. HEALTH AND HUMAN SERVICES COORDINATION

The FCC and HHS have established an on-going dialogue related to emergency preparedness and response with a focus on the respective agencies' outreach programs and Operations Center activities as part of the overall effort to assist hospitals, emergency medical services, and local communities during public-health emergencies. In early 2009, a senior FCC delegation met with the Office of the Assistant Secretary for Preparedness and Response to discuss, among other things, the FCC's experiences assisting healthcare entities following Hurricane Ike, lanes of jurisdiction between the two agencies, and opportunities for closer collaboration. FCC officials had previously visited the HHS Secretary's Operation Center.

Solution—Discussions about the potential for establishing an informal communications working group with HHS, including its Centers for Disease Control and Prevention and other Federal agencies such as DHS, are underway. A meeting between PSHSB Chief Barnett and HHS Assistant Secretary for Preparedness and Response Dr. Kevin Yeskey has been scheduled for September 15, 2009. Establishment of a working group of FCC and HHS personnel would be in order given the need, for example, to coordinate public communications requirements during a pandemic outbreak as the load on communications networks skyrockets.

5. EMERGENCY ALERT SYSTEM

Concerns have been raised regarding the frequency and scope of EAS testing.

Solution—The FCC is working with Federal partners at FEMA, NOAA, and the Executive Office of the President to identify ways to enhance the national EAS, to ensure that the American public receives national emergency alerts in a timely fashion. Two meetings have occurred already and more are scheduled.

6. CYBER SECURITY ENGINEERING EXPERTISE/CYBER SECURITY WORKING GROUP

As the White House's recent Cyberspace Policy Review Report points out, "the globally-interconnected digital information and communications infrastructure known as 'cyberspace' underpins almost every facet of modern society and provides critical support for the U.S. economy,

civil infrastructure, public safety, and national security." Consequently, the Report stresses that Federal departments and agencies should focus on the importance of cyber security with respect to their operations.

Solution—The FCC has established a Cyber Security Working Group to assess the FCC's current cyber security expertise and assets, identify the FCC's needs and requirements for cyber security expertise (including a consideration of the FCC's role in cyber security), identify gaps and vulnerabilities, and develop recommendations to address the deficiencies. The working group already has met and will provide the Chairman with a report by the end of November.

7. COOP AND PANDEMIC PLANS

With the influx of new leadership, FCC COOP and Pandemic Plans must be updated to reflect personnel changes.

Solution—The FCC COOP Plan and Pandemic Plans have been reviewed and updated, and were approved by PSHSB Chief Barnett on September 4, 2009.

8. EMERGENCY COMMUNICATIONS PLANNING INFORMATION-PSHSB WEBSITE

The FCC website can be an excellent resource for state, tribal, and local governments, communications service providers, hospitals, and the public safety community to find emergency information, technical planning guidance, and contact information.

Solution—The FCC will re-align resources to ensure that more critical emergency information is available faster, with more accessibility on the PSHSB website.

9. EMERGENCY OUTREACH NOTIFICATION CAPABILITY

At the outset of a major disaster, FCC Operations Center personnel make calls to large numbers of 9-1-1 centers, hospitals, and state and local emergency operations centers to provide emergency contact information and to let them know who to contact should their essential communications systems fail during the impending disaster. Because of the large volume of calls that must be made and the short time to make them, some of the essential state and local emergency entities cannot be contacted prior to the event. In addition, the current process is very labor intensive and takes the watch officers away from other essential tasks related to the FCC's emergency response.

Solution—Procure a notification system that will allow rapid notification of state and local public safety and emergency organizations during emergencies via phone and e-mail, as well as enable rapid notification and assembly of FCC emergency management and COOP staff. The Chairman has ordered the PSHSB to equip the Operations Center with a notification system that will allow rapid notification of state, tribal, and local public safety and emergency organizations via phone and e-mail, as well as enable rapid notification and assembly of FCC emergency management and COOP staff.

10. CONTINUITY OF OPERATIONS AND SHELTER IN PLACE TRAINING AND PROCEDURES

A need for additional employee training for COOP and Shelter in Place has been identified.

Solution—PSHSB should prepare and implement a plan to develop and publish the necessary planning materials for the FCC's emergency personnel in all Bureaus and Offices, as well as general information regarding the FCC's emergency plans for all FCC employees. OMD and PSHSB also will provide training in COOP and shelter-in-place for all FCC employees and a COOP exercise for senior managers.

The Chairman has directed OMD and PSHSB to develop training modules that will introduce FCC employees to COOP and shelter-in-place procedures. These modules will explain what employees should expect during a crisis situation. The working group has met, assigned actions items to its members, and is nearing completion of the project.

11. COMMUNICATIONS, SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL

Earlier this year, the FCC established a new advisory committee known as the Communications Security, Reliability, and Interoperability Council or CSRIC. This Council is to focus on emergency communications issues including: recommending best practices and actions the FCC can take to ensure the security, reliability, operability, and interoperability of public safety communications systems; recommending best practices and actions the FCC can take to improve the reliability and resiliency of communications infrastructure; evaluating ways to strengthen the collaboration between communications service providers and public safety entities during emergencies and making recommendations for how they can be improved; developing and recommending best practices and actions the FCC can take that promote reliable 911 and enhanced 911 (E911) service; analyzing and recommending technical options to enable accurate and reliable dynamic E911 location identification for interconnected Voice over Internet Protocol (VoIP) services; recommending ways, including best practices, to improve EAS operations and testing and to ensure that all Americans, including those living in rural areas, the elderly, persons with disabilities, and persons who do not speak English, have access to timely EAS alerts and other emergency information; recommending methods to measure reliably and accurately the extent to which key best practices are implemented both now and in the future; and making recommendations with respect to such additional topics as the FCC may specify.

Solution—Seat and call to order the initial CSRIC panel.

12. PROJECT ROLL CALL SPECTRUM MONITORING UNITS

The FCC partners with FEMA in the use of Project Roll Call signal analysis equipment. The FCC, however, may wish to use Project Roll Call for its own responsibilities.

Solution—The FCC will purchase and deploy its own Project Roll Call equipment.

13. PSHSB EMERGENCY PROCEDURES

PSHSB acts as the primary source of outside warnings and alerts. When these messages are received, it is the Bureau's responsibility to confirm the information and provide it to FCC management. A review revealed that some improvements could be made in this area.

Solution—PSHSB is in the process of updating and revising all of its standard operating procedures related to alerts and warnings, and is training its watch officers on these procedures. In addition, PSHSB will establish a process to review and update all standard operating procedures twice a year. This process will include a complete review of the list of FCC managers that should receive the alerts.

14. DEVOLUTION TEAM DEVELOPMENT AND TRAINING

A review found that the FCC's Devolution Team needs more training and exercise.

Solution—Training and exercises for the Devolution Team will be accelerated and made more robust.

15. IT-BASED EMERGENCY RESPONSE SYSTEMS TRAINING

PSHSB has IT-based systems that offer important functionalities that can improve the FCC's incident management for major disasters. Additional training is necessary for the full implementation of these systems.

Solution—PSHSB will develop and provide training and annual updates on these systems for FCC emergency personnel.

16. VPN AND BANDWITDH

It is important that key staff and managers have robust, high-speed remote access to the FCC's computer network and the essential databases. This is especially important should the FCC implement its pandemic plan. For a pandemic outbreak, the Department of Health and Human Services projects that absenteeism could be close to forty percent of the workforce and telework would be increased dramatically.

Solution—PSHSB has been working with OMD staff on potential VPN solutions and associated funding requirements.

17. SATELLITE COMMUNICATIONS TRAINING FOR EMERGENCY RESPONDERS

During major disasters, terrestrial communications systems often suffer severe damage that eliminates much of the emergency communications capability within the disaster area for a considerable time. During such instances, the use of satellite-based systems should be considered to restore vital communications links.

Solution—Provide training in emergency satellite communications systems for FCC staff members who will be assigned to emergency response teams in the field.

18. OUTAGE REPORTING ON IP-BASED COMMUNICATIONS SYSTEMS

Part 4 of the FCC's rules regarding the reporting of disruptions to communications services does not apply to IP-based communications that have become increasingly important as substitutes for, and complements to, older communications services. The continued safety, security, and economic well-being of the public depend on the continued reliability and integrity of communications services that are migrating to these IP networks.

Solution—The FCC will conduct a workshop to discuss issues related to IP-based communications disruptions that impact interconnected VoIP services and the growing number of communications services that rely on broadband ISPs.

19. EB EQUIPMENT DEVELOPMENT GROUP (EDG)

The review noted some outstanding requirements pertaining to EB's EDG facility.

EB's fleet of direction finding vehicles and PSHSB's HFDFC equipment is dependent on the highly-specialized work done by this group. This ability to design, manufacture, and integrate custom electronics, software and mechanical hardware allows the field offices and the HFDFC flexibility to obtain original technical solutions within a short period for their diverse needs. During an event, EDG prepares, ships, and deploys spare equipment to support the deployed EB agents, offers in-house technical equipment to loan, and effectuates repairs to FCC equipment.

Solution—EB has identified requirements necessary to ensure that EDG can perform its mission.

20. EB FIELD DEPLOYMENT STAFFING

The review noted some outstanding resource requirements related to EB's field offices.

Solutions—EB has identified requirements necessary to ensure that its field offices can perform their duties.

21. RULES FOR PRIORITY SERVICES

The FCC's rules for Telecommunications Service Priority (TSP) and Wireless Priority Service (WPS) programs have not been updated in over twenty-one and ten years, respectively. During that span, significant changes to the underlying technology and market usage have transpired and numerous problems have been identified that jeopardize the efficacy of these programs. The FCC's rules need to be updated.

Solution—The FCC will conduct a workshop to discuss issues related to improving the efficacy of these programs in light of developments in technology and market usage.

SECTION 8: OUTSIDE EVALUATIONS & CRITIQUES

8. What outside critiques and evaluations have been made of the FCC's handling of emergency situations and incidents? (e.g., GAO, Inspector General, industry analysts, media, other government entities)

Generally, the FCC has received high marks for its efforts following Hurricane Katrina, its preparedness actions after Hurricane Katrina, and its recovery efforts during the 2008 Hurricane Season. Other agencies, such as FEMA, have complimented the FCC's efforts, particularly in light of creative solutions developed such as Project Roll Call. In the White House Lessons Learned document issued after Hurricane Katrina, the FCC is listed in the section "What Went Right" and is cited for acting quickly to facilitate the resumption of communications services in affected areas and to authorize the use of temporary communications services for use by emergency personnel and evacuees in shelters.[19]

Here are a few other examples of the notable acknowledgements for the FCC's commendable efforts relating to Katrina:

> "[O]ne thing I should have pointed out, that helped a great deal, is the quick reaction from the FCC. There were some things we did, to start porting numbers that normally would not have been allowed. The FCC acted quickly in that regard, so I commend them for their help."

Testimony of Bill Smith, Chief Technology Officer, BellSouth to the Senate Commerce, Science and Transportation Committee (September 22, 2005).

> "I want to express my thanks to Chairman Martin, Commissioners Abernathy, Adelstein and Cotts (sic) and the staff of the FCC. Their efforts greatly assisted America's satellite companies in restoring telecommunications services to the Gulf Coast region."

Testimony of Tony Trujillo Jr., Satellite Industry Association to the Senate Commerce, Science and Transportation Committee (September 29, 2005).

[19] *See* Appendix B of *The Federal Response to Hurricane Katrina: Lessons Learned* (2006) at http://georgewbush-whitehouse.archives.gov/reports/katrina-lessons-learned.pdf.

> "[T]he FCC stepped up in leadership and authority as a clearinghouse for telecommunication recovery needs."

Testimony of Hossein Eslambolchi, President, AT&T Global Networking Technology Services, Chief Technology Officer and Chief Information Officer, AT&T Labs to the Senate Commerce, Science and Transportation Committee (September 29, 2005).

> "'The FCC performed in exemplary fashion in its response,' said Tom Taylor, editor of Inside Radio, the gold standard of radio industry publications. They really showed what a responsive federal agency can do in terms of offering sensible support to an infrastructure that badly needed help (like expedited permission to stay on extra hours). They literally had staff in there seven days a week and (this is particularly impressive to me) they *called* (emphasis original) every radio (and I guess TV) station along the Gulf Coast, reaching out to see what the situation was."

Editorial, by Dimitri Vassilaros, Pittsburgh Tribune-Review, August 28, 2006 at http://www.pittsburghlive.com/x/pittsburghtrib/opinion/columnists/vassilaros/s_467743.html.

The FCC's Katrina Panel observed significant impediments to the recovery effort resulting from:

- Inconsistent and unclear requirements for communications infrastructure repair crews and their subcontractors to gain access to the affected area.
- Limited access to power and/or generator fuel.
- Limited security for communications infrastructure and personnel.
- Lack of pre-positioned back-up equipment.
- Lack of established coordination between the communications industry and state and local officials as well as among federal, state and local government officials with respect to communications matters.
- Limited use of available priority communications services, such as GETS, WPS, and the TSP.

The Katrina Panel made note of the numerous actions taken by the FCC to support communications service providers in their recovery efforts, and found that these actions appeared to assist substantially providers in their efforts. It noted, however, that while communications providers were generally clear that the FCC was the correct agency to contact for regulatory relief after the disaster, many providers were unclear as to which agencies to contact for other types of Federal assistance (e.g., fuel authorizations, access to impacted area).[20] The Katrina Panel also found that communications providers often could not determine which Federal agency was responsible for implementing important recovery programs or distributing resources to communications companies operating in the impact area. It also noted that repeated and competing requests for outage information from Federal, state, and local government entities added to the confusion

[20] *See Katrina Panel Report and Recommendations to the FCC* (June 12, 2006) at 21 FCC Rcd 7,320, Appendix B at 20 (http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-83A1.pdf).

about agency roles and resulted in distractions to communications provider personnel engaged in recovery efforts.[21]

On June 12, 2006, the Katrina Panel submitted a report that included a number of recommendations designed to enhance the FCC's emergency response efforts as well as those of the communications industry and the public safety community. On June 19, 2006, the FCC initiated a comprehensive rulemaking to address and implement the Katrina Panel's recommendations. On June 8, 2007, the FCC released an order directing the PSHSB to implement several of the emergency preparedness/response-related Katrina Panel recommendations.

Currently, the GAO is examining issues of Emergency Communications, EAS, and Pandemics and the Financial Industry. The first examination will focus on the relationship of the FCC and DHS's Office of Emergency Communications, the second will focus more on FEMA, and the third looks at assuring communications for the financial industry during a crisis. These reports have not been issued (PSHSB reviewed a draft of the report on Emergency Communications and EAS). The GAO has also instituted a review of the NCS and its programs, with which the FCC has some engagement. No date has been set for the release of the GAO NCS report.

[21] *Id.*